Electronic Version
Stylesheet Version v1.1.1

# METHOD FOR MANAGING A BUFFER MEMORY IN A CRYPTO ENGINE

## Abstract

A method for managing a buffer memory in a crypto engine includes defining an IO writing address, a program reading address, a program writing address, and an IO reading address in the buffer memory. Input data is written into the IO writing address, and then the crypto engine reads the input data beginning at the program reading address to perform encryption or decryption processes. After the encryption or decryption processes, result of the processes is written into the program writing address, and then the result is read beginning at the IO reading address. When the IO writing address is different from the program reading address, the crypto engine is controlled to read the input data. When the program writing address is different from the IO reading address, the buffer memory is controlled to output the result.